ROBBINS GELLER RUDMAN
& DOWD LLP
SHAWN A. WILLIAMS (213113)
MATTHEW S. MELAMED (260272)
JOHN H. GEORGE (292332)
ARMEN ZOHRABIAN (230492)
Post Montgomery Center
One Montgomery Street, Suite 1800
San Francisco, CA 94104
Telephone: 415/288-4545
415/288-4534 (fax)
shawnw@rgrdlaw.com
mmelamed@rgrdlaw.com
jgeorge@rgrdlaw.com

Lead Counsel for Lead Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

In re ZOOM SECURITIES LITIGATION This Document Relates To: ALL ACTIONS.	Case No. No. 2:20-cv-02353-JD CONSOLIDATED CLASS ACTION COMPLAINT FOR VIOLATION OF THE FEDERAL SECURITIES LAWS DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Page

Page

I. INTRODUCTION

1. Lead Plaintiff Adam M. Butt ("Plaintiff"), individually and on behalf of all others similarly situated, by Plaintiff's undersigned attorneys, alleges the following, based upon personal knowledge as to Plaintiff and Plaintiff's own acts, and upon information and belief as to all other matters, based on the investigation conducted by and through Plaintiff's attorneys, which included, among other things, a review of Zoom Video Communications, Inc.'s ("Zoom" or the "Company") press releases, website, United States Securities and Exchange Commission ("SEC") filings, analyst reports, media reports and other publicly disclosed information about Defendants (defined herein). Plaintiff believes that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

2. This is a securities fraud class action alleging violations of the anti-fraud provisions of the federal securities laws on behalf of all who purchased or acquired Zoom securities from April 18, 2019 through April 6, 2020, inclusive (the "Class Period"). The claims asserted herein are brought against Zoom and two of its officers: Eric S. Yuan ("Yuan"), the Company's founder, Chairman of the Company's Board, the Company's Chief Executive Officer ("CEO") and President, and Kelly Steckelberg ("Steckelberg"), the Company's Chief Financial Officer ("CFO").

3. During the Class Period, Defendants violated §§10(b) and 20(a) of the Securities Exchange Act of 1934 ("Exchange Act"), 15 U.S.C. §§78j(b) and 78t(a), and Rule 10b-5 promulgated thereunder, 17 C.F.R. §240.10b-5, by making false and misleading statements and omissions concerning the Company's operations; the security capabilities, including the ability to use AES 256-bit end-to-end encryption, available in its main product offering, Zoom Meetings; and its collection and use of its users' personal data.[1]

II. BACKGROUND AND SUMMARY OF THE ACTION

4. Zoom, founded in 2011, describes itself as a provider of a video-first communications platform that delivers happiness and fundamentally changes how people interact by connecting people through frictionless video, voice, chat and content sharing and enabling face-to-face video

[1] Plaintiff attaches hereto as Exhibit A its securities fraud allegations in chart form.

experiences for thousands of people in a single meeting across disparate devices and locations. The Company states that its cloud-native platform delivers reliable, high quality video that is easy to use, manage and deploy; provides an attractive return on investment; is scalable; and easily integrates with physical spaces and applications.

5. Zoom Meetings ("Zoom Meetings"), the Company's main product and its platform for individual or group videoconferences, is the "cornerstone" around which the Company provides a suite of products and features designed to give users a frictionless communications experience.[2] Users of Zoom's products include both hosts who organize video meetings and individual attendees who participate in meetings. Zoom conducted its initial public offering ("IPO") on April 18, 2019.

6. During the Class Period, beginning with its IPO, Zoom falsely asserted, among other things, that communications using Zoom Meetings could be secured with end-to-end encryption. Specifically, in Zoom's registration statement and prospectus, filed in connection with its April 18, 2019 IPO, and its Security Guide,[3] featured prominently on its website on that date, Defendants falsely touted, for meetings on its platform, that end-to-end encryption was part of the Company's currently available security capabilities:

- "The ***following in-meeting security capabilities are available*** to the meeting host: ***Secure a meeting with end-to-end encryption (E2E)***";
- "***We offer robust security capabilities, including end-to-end encryption***";
- "***End-to-end encryption [is available] for all meetings***"; and
- Zoom users could "***Secure a meeting with end-to-end encryption (E2E)***" and "***Enable end-to-end encrypted meetings***" using "Advanced Encryption Standard (AES) 256-bit algorithm."

[2] In addition to Zoom Meetings (including Zoom Chat), the Company's products include: Zoom Rooms, Zoom Conference Room Connector, Zoom Phone, Zoom Video Webinars, Zoom for Developers and Zoom App Marketplace. Zoom Phone is a cloud-based private branch exchange system, while Zoom Rooms is a software-based conference room system that enables users to experience Zoom Meetings in physical meeting spaces.

[3] Since March 2016, at the latest, Zoom published security white papers titled "Security Guide" "to provide information on the security features and functions that are available with Zoom."

Defendants repeated substantially identical misrepresentations concerning Zoom Meetings' purported ability to provide end-to-end encryption throughout the Class Period. *See* ¶¶27, 30, 32, 39, 42-43.

7. Investment analysts who covered the Company credited Zoom's use of end-to-end encryption as a "key strength," a "KEY PLATFORM FEATURE" and a "major source[] of competitive differentiation."

8. In addition, throughout the Class Period, Defendants published Zoom's Privacy Policy in connection with its Zoom Meetings suite of products purporting to inform its users about the manner in which it collected and used their personal data:

> We may ***collect***, either as Controller or Processor, the following categories of Personal Data about you when you use or otherwise interact with our Service: . . . Facebook profile information (***when you use Facebook to log-in to our Products or to create an account for our Products)***.[4]

9. In truth, however, each of the statements concerning Zoom's security capabilities, such as the use of AES 256-bit end-to-end encryption, and Defendants' collection and usage of its users' data as detailed in Defendants' Privacy Policy, was materially false and misleading when made because Defendants knew or deliberately disregarded and failed to disclose the following facts:

(a) Zoom Meetings were ***not*** secured with end-to-end encryption. Whereas end-to-end encryption means that not even the company that runs the messaging service can access the cryptographic keys necessary to decrypt the end users' communication, here Zoom secretly maintained access to the cryptographic keys that could allow Zoom to decrypt and decipher the communications between the end users, thereby breaking the "end-to-end promise."[5] Nor did Zoom

---

[4] Zoom made substantially similar misrepresentations in its Privacy Policy dated March 19, 2019, December 31, 2019, February 23, 2020 and March 18, 2020.

[5] End-to-end encryption has the following known and accepted definition in the tech industry:

> [A] system of communication where the only people who can read the messages are the people communicating. No eavesdropper can access the cryptographic keys needed to decrypt the conversation – not even a company that runs the messaging service.
>
> * * *

use AES 256-bit encryption to secure the content of communications between users of Zoom Meetings. Rather, Zoom used AES 128-bit encryption, a lower level of encryption that provides less secure protection of users' communications.

(b) Zoom was not just ***collecting*** its users' personal data but was also ***sending*** that personal data to Facebook, including data from Zoom users who did not have a Facebook account, without their consent or notification.

(c) Zoom users who subscribed to the LinkedIn Sales Navigator feature were able to view links to the publicly available LinkedIn profiles of ***other*** meeting participants, without their consent or notification, including those participants had ***not*** signed up for the LinkedIn Sales Navigator feature. This functionality even worked to display the LinkedIn profiles of users who adopted pseudonyms in Zoom Meetings in order to remain anonymous, which resulted in their real names being disclosed to participants who subscribed to a LinkedIn feature despite Zoom's guidance indicating that users could control how their names appeared.

10. In addition, while Zoom and the Individual Defendants had, in its registration statement and prospectus, characterized the Company as one that put a high priority on security and data privacy, Zoom intentionally and covertly installed a web server on Zoom's users' Mac computers that the Company had "consciously" engineered to bypass security settings on the Mac-native internet browser Safari. The web server that Zoom covertly installed on Mac users' computers permitted the computer's camera to be turned on remotely without the users' consent and remained on users' Mac computers even after users deleted the Zoom app.

11. On July 8, 2019, a software security engineer disclosed that Zoom was covertly installing a local web server on Mac users' computers, that its installation permitted Mac users' cameras to be turned on remotely without the users' consent and that the server remained on Mac

---

> That "end-to-end" promise means that messages are encrypted in a way that allows only the unique recipient of a message to decrypt it, and not anyone in between. In other words, only the endpoint computers hold the cryptographic keys, and the company's server acts as an illiterate messenger, passing along messages that it can't itself decipher.

Andy Greenberg, *Hacker Lexicon: What Is End-to-End Encryption?*, Wired (Nov. 25, 2014), https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

users' computers even if users deleted the Zoom app. Following this partial disclosure, Zoom's stock price declined $1.12 per share, from $91.88 at the close of the prior trading day to $90.76.

12. Nevertheless, the other material representations and omissions continued to cause the Company's stock price to trade at artificially inflated prices, which reached as high as $164.94 on March 23, 2020.

13. Then, in late March 2020 and continuing into early April 2020, a series of disclosures and admissions by or about Defendants incrementally revealed the previously concealed facts concerning Zoom's knowing or reckless failure to protect the personal data and privacy of its users' communications on Zoom's platform in accordance with representations made to the public, its users and the investment community:

- March 26, 2020: The website Motherboard published an article disclosing that Zoom not only collected users' data but ***sent users' data to Facebook***, including data from Zoom users who did not have a Facebook account.
- March 30, 2020: *The New York Times* published an article disclosing that the New York Attorney General was investigating Zoom for its security and privacy practices, including the data it collected from users and the entities to whom it sent users' data.
- March 31, 2020: *The Intercept* published an article disclosing that Zoom Meetings did ***not*** offer end-to-end encryption and quoted a Zoom spokesperson admitting that: "Currently, it is not possible to enable E2E [end-to-end] encryption for Zoom video meetings."
- April 1, 2020: Defendants published a blog post admitting that Zoom Meetings were ***not*** end-to-end encrypted and apologizing for "incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption."
- April 2, 2020: *The New York Times* published an article disclosing that "a data-mining feature on Zoom allowed some participants to surreptitiously have access to LinkedIn profile data about other users – without Zoom asking for their permission.
- April 3, 2020: Citizen Lab, an interdisciplinary laboratory at the University of Toronto, issued a report disclosing that Zoom Meetings were ***not*** encrypted using AES-256 encryption but rather with weaker AES-128 encryption.
- April 4, 2020: *The Wall Street Journal* published an interview with CEO Yuan stating that end-to-end encryption would not be available for at least a few months.
- April 6-8, 2020: Zoom systematically scrubbed a series of articles on Zoom's website, deleting all references to the availability of "end-to-end" encryption.

14. Each of these disclosures of the facts concerning the Company's true business condition, beginning with the March 30, 2020 article published in *The New York Times*, individually and in the aggregate caused the Company's stock price to decline precipitously as the artificial inflation induced by the misrepresentations and omissions began to dissipate. Investment analysts attributed the price declines to the newly disclosed information concerning the security and privacy flaws. For example, on March 31, 2020, Benzinga reported that "shares of Zoom Video Communications dropped 6.14%," attributing the decline to *The New York Times*' reporting of the privacy and security probes from the New York Attorney General. On April 2, 2020, CNBC reported that "shares of Zoom cratered" 11% after the Company's CEO apologized for security lapses. On April 6, 2020, *Fortune* published an article that stated: "Zoom stock dropped as much as 14.5% this morning, after concerns over the security of the company's video-chat and meeting software led to several major organizations banning or discouraging its use."

15. All told, Zoom's stock price declined in response to these disclosures, which incrementally and in the aggregate revealed the true state of affairs, falling from a closing price of $150.88 per share on March 30, 2020 to $113.75 on April 7, 2020 – ***a decline of 25%*** – as the artificial inflation resulting from Defendants' false and misleading statements was removed from the share price. *See infra* §IX.

16. Following these disclosures, federal regulators began investigating Zoom. On November 9, 2020, Zoom entered a proposed consent agreement with the U.S. Federal Trade Commission ("FTC") requiring the Company to implement robust information security programs to settle charges that Zoom engaged in deceptive and unfair practices that undermined the security of its users. The FTC charged Zoom with, among other matters: falsely or misleadingly representing that it employed AES 256-bit end-to-end encryption; and deceptively deploying a web server (that remained on users' computers even after they had uninstalled the Zoom app) that circumvented Safari's privacy and security safeguards without providing notice to or obtaining consent from its users.

17. On December 18, 2020, Zoom disclosed that the U.S. Department of Justice's ("DOJ") U.S. Attorney's Office for the Eastern District of New York had issued grand jury

subpoenas seeking information regarding, among other matters, the development and implementation of Zoom's Privacy Policies. Similarly, Zoom disclosed that the U.S. Attorney's Office for the Northern District of California and the SEC had issued subpoenas seeking information regarding, among other matters, "various security and privacy matters, including Zoom's encryption, and Zoom's statements."

18. Members of the putative class seek to recover their economic losses as a result of the conduct alleged herein.

III. JURISDICTION AND VENUE

19. The claims asserted arise under §§10(b) and 20(a) of the Exchange Act, 15 U.S.C. §78j(b) and 78t(a) and Rule 10b-5, 17 C.F.R. §240.10b-5. Jurisdiction is conferred by, and venue is proper pursuant to, §27 of the Exchange Act, 15 U.S.C. §78aa. The Company's headquarters are in San Jose, California, false statements were made in this District and acts giving rise to the violations complained of occurred in this District.

IV. THE PARTIES

20. Lead Plaintiff Adam M. Butt purchased or acquired Zoom common stock during the Class Period and was damaged by the conduct alleged herein.

21. Defendant Zoom, a Delaware corporation headquartered in San Jose, California, provides a platform for video, voice, content sharing and chat that runs across mobile devices, desktop computers, telephones and internet-connected systems. Zoom's common stock is listed and trades on the NASDAQ, an active market, under the ticker symbol "ZM."

22. Defendant Yuan, also known as Zheng Yuan, is Zoom's founder and has served as the Chairman of the Company's Board, as President and as CEO since June 2011. As CEO, Yuan was regularly quoted in Zoom's press releases and regularly spoke on Zoom's quarterly earnings calls with Wall Street analysts and investors. Yuan also signed or authorized the filing of Zoom's reports filed with the SEC. Yuan holds a bachelor's degree in applied math from Shandong University of Science and Technology and a master's degree in engineering from China University of Mining and Technology. Prior to founding Zoom, Yuan was one of the founding engineers and worked at WebEx, a web conferencing and videoconferencing platform that was acquired by Cisco

Systems in 2007. When WebEx was acquired, Yuan became Cisco's Corporate Vice President of Engineering.

23. Defendant Steckelberg has served as the Company's CFO since November 2017. Since becoming Zoom's CFO, Steckelberg had the power to authorize or approve publicly disseminated information about the Company, regularly spoke on Zoom's quarterly earnings calls with Wall Street analysts and investors, made live presentations at analyst-sponsored investor conferences and signed or authorized filings for Zoom with the SEC.

24. Defendants named in ¶¶22-23 are referred to as the "Individual Defendants." Zoom and the Individual Defendants are collectively referred to herein as "Defendants."

V. CONTROL PERSONS

25. The Individual Defendants, because of their positions with the Company, individually and collectively possessed the power and authority to control the contents of Zoom's reports to the SEC; press releases; and public presentations to securities analysts, money portfolio managers and institutional investors. The Individual Defendants were provided with copies of the Company's reports, press releases and articles alleged herein to be misleading prior to or shortly after their issuance and had the ability and opportunity to prevent their issuance or cause them to be corrected. The Individual Defendants participated in drafting, preparing, disseminating and/or approving the various documents and other communications alleged to be false and misleading herein. Because of their positions within the Company, and their access to material non-public information available to them but not to the public, the Individual Defendants knew that the adverse facts specified herein had not been disclosed to and were being concealed from the public and that the positive representations being made were then materially false and misleading. The Individual Defendants are liable for the false and misleading statements and omissions pled herein. Additionally, because of their positions of control and authority as officers or directors of the Company, the Individual Defendants were able to and did control the content of the various SEC filings, press releases and other public statements pertaining to the Company during the Class Period. Zoom has stated that if the Company lost the services of its senior management, *e.g.*, the Individual Defendants, the Company may not be able to execute its business strategy.

VI. FALSE AND MISLEADING STATEMENTS DURING THE CLASS PERIOD

A. Defendants' April and June 2019 Materially False and Misleading Statements Regarding Encryption, Security and Data Privacy

26. On April 18, 2019, Zoom filed its prospectus (part of the Company's registration statement) with the SEC pursuant to SEC Rule 424(b)(4) and offered 20,869,565 shares at $36.00 per share in the Company's IPO, raising more than $750 million.

27. Defendants' April 18, 2019 prospectus falsely touted end-to-end encryption as a key aspect of the robust security capabilities of the Company's offerings, including Zoom Meetings:

> ***Security and disaster recovery. We offer robust security capabilities, including end-to-end encryption***, secure login, administrative controls and role-based access controls.

28. Zoom's Privacy Policy dated March 19, 2019, which remained featured on its website at zoom.us/privacy on April 18, 2019, falsely asserted that the Privacy Policy outlined the Company's collection and use of personal data:

> [Zoom] is committed to protecting your privacy and ensuring you have a positive experience on our website and in using our products and services. This policy covers the Zoom website zoom.us, mobile applications, and desktop clients and is applicable worldwide.
>
> ***This policy outlines our handling practices and how we collect and use the Personal Data you provide during your online and offline interactions with us***.

29. The March 19, 2019 Privacy Policy also falsely stated that:

> We may ***collect***, either as Controller or Processor, the following categories of Personal Data about you when you use or otherwise interact with our Service: . . . ***Facebook profile information (when you use Facebook to log-in to our Products or to create an account for our Products)***.

30. In addition to representations in the Company's registration statement and prospectus, the Company also featured, as of April 18, 2019, several articles and blogs on its website at blog.zoom.us that falsely stated Zoom's videoconferencing technology was secured with "AES 256-bit end-to-end encryption." The blog posts further detail the importance of end-to-end encryption to Zoom's consumers in numerous industries, including technology, healthcare and financial:

- *Introducing Zoom for Telehealth* and *Zoom Reporting Live from American Telemedicine Association 2017*, respectively: "Zoom for Telehealth includes the

following features pre-configured: . . . ***[e]nd-to-end AES-256 bit encryption*** of all meeting data and instant messages."

- *Zoom Feature Spotlight: Linux Client*: "Let's look at some ***key features*** of the Zoom Linux platform: . . . ***[e]nterprise-grade security with AES-256 bit end-to-end encryption***."

- *Zoom Partners with OpenExchange to Provide Video Communications for Financial Services Market*: "The partnership of our video services offers numerous benefits to customers, including: . . . ***[s]ecure cloud (and optional hybrid cloud/on-prem) communications environment with AES-256 bit end-to-end encryption***."

- "***End-to-End Encrypted*** Zoom Allows FINRA to Maintain a High-Security Posture."

31. In May 2019, five investment firms initiated analyst coverage of the Company with reports noting the core importance of the purported fact that Zoom's videoconferencing technology was secured with end-to-end encryption, referring to it as a "key strength," a "KEY PLATFORM FEATURE[]" and a "major source[] of competitive differentiation," as reflected in the following excerpts:

- May 13, 2019 Bank of America Report: "***Zoom has enterprise level security and compliance features, including end to end encryption***, secure log-in, role-based access controls, and many more."

- May 13, 2019 JMP Report: "Below we discuss the key strength of Zoom's technology and infrastructure, as well as key strengths of its cloud-native infrastructure. . . . *Security and disaster recovery:* ***The company offers robust security capabilities, which include end-to-end encryption***, secure login, administrative controls, and role-based access controls."

- May 13, 2019 PiperJaffray Report: "KEY PLATFORM FEATURES . . . [s]ecurity and disaster recovery . . . ***[e]nd-to-end encryption***, secure login, and role-based access controls to ensure secure communications."

- May 13, 2019 RBC Report: "We feel that core features of the company's technology and the major sources of competitive differentiation include: . . . ***Zoom has end-to-end encryption capabilities to ensure that data streams are protected from outsiders and not disrupted***."

- May 23, 2019 Oppenheimer Report: "Last, Zoom's proprietary algorithms optimize connectivity and service quality by detecting packet loss and latency while supporting multi-bitrate encoding (vs. standard rate transcoding) ***offering robust security functionality (end-to-end encryption***, secure login, and disaster recovery)."

32. In June 2019, Zoom updated its Security Guide, which it posted on its website and subsequently referred to in other public communications.[6] The June 2019 Security Guide described its purpose as "provid[ing] information on the security features and functions that are available with Zoom" and stated that: "Unless otherwise noted, the security features in this document apply across the product suite of Zoom Meetings, Zoom Video Webinars, Zoom Rooms, and Zoom Voice, across supported mobile, tablet, desktop, laptop, and SIP/H.323 room system endpoints." The June 2019 Security Guide falsely represented that the Company' pre-meeting and in-meeting security capabilities included the ability for Zoom Meetings users to enable end-to-end encryption:

The following pre-meeting security capabilities are available to the meeting host:

- ***Enable an end-to-end (E2E) encrypted meeting***.

* * *

The following in-meeting security capabilities are available to the meeting host:

- ***Secure a meeting with E2E encryption***.

33. By July 5, 2019, Zoom's stock price had increased from the IPO price of $36.00 per share to close at $91.88.

B. Reasons Defendants' April and June 2019 Material Misrepresentations Regarding Encryption, Security and Privacy Were Made Knowingly or with Deliberate Recklessness

34. Each of Defendants' statements in ¶¶27-30 and 32 concerning Zoom's purported security capabilities, including the availability of end-to-end AES 256-bit encryption, and its Privacy Policy, which purported to outline the Company's data collection and handling, was materially false and misleading when made, as Defendants knew or deliberately disregarded and failed to disclose the following facts:

(a) Zoom Meetings were not in fact secured with end-to-end encryption. Instead, Zoom maintained access to the cryptographic keys for Zoom Meetings such that they could decrypt and decipher the communications between end users. Whereas end-to-end encryption means that not even the company that runs the messaging service can access the cryptographic keys necessary to

[6] The Zoom Security Guides on Zoom's website were dated with month and year only.

decrypt the end users' communications, here Zoom maintained access to the cryptographic keys that could allow Zoom to decrypt and decipher the communications between the end users, thereby breaking the "end-to-end promise." Zoom's servers were therefore not an illiterate messenger, and Zoom could decipher the messages that it passed between users. Defendants knew the meaning of end-to-end encryption; and, in fact, they used the term accurately in other contexts, including in describing Zoom's end-to-end chat encryption in the Company's security white papers.[7] Further, Yuan himself led the effort to engineer Zoom Meetings' platform and is named on several patents that specifically concern encryption techniques.[8] Nor did Zoom use AES 256-bit encryption to secure the content of communications between users of Zoom Meetings. In truth, Zoom used AES 128-bit encryption, a lower level of encryption, to encrypt and decrypt audio and video in Zoom Meetings. AES 128-bit encryption provides less secure protection of users' communications than AES 256-bit encryption.

(b) While Zoom's Privacy Policy disclosed that the Company may ***collect*** users' personal data "when [users] use Facebook to log-in to our Products or to create an account for our Products," it failed to disclose that Zoom was surreptitiously sending users' data to Facebook – including from users who did not have a Facebook account – without users' consent or notification. Notably, Facebook required that developers that use its software development kit ("SDK"), such as Zoom, be transparent with users about the data their apps send to Facebook. ¶49.

(c) When users signed into a meeting, Zoom's software automatically and surreptitiously sent their names and e-mail addresses to a company system it used to match them

---

[7] Zoom's June 2019 Security Guide stated: "E2E Chat Encryption: Zoom E2E chat encryption allows for a secured communication where only the intended recipient can read the secured message. Zoom uses public and private key to encrypt the chat session with Advanced Encryption Standard (AES-256). Session keys are generated with a device-unique hardware ID to avoid data being read from other devices. This ensures that the session can not be eavesdropped on or tampered with."

[8] *See* U.S. Patents 8,078,676 (dated December 13, 2011; filed August 6, 2004), 8,417,801 (dated April 9, 2013; filed November 9, 2011) and 8,578,465 (dated November 5, 2013; filed July 21, 2009). Patents 8,078,676 and 8,417,801 involve using "suitable encryption techniques, such as Secure Sockets Layer (SSL) encryption" to encrypt data during transfer, while Patent 8,578,465 discusses using further encryption algorithms, stating that: "The ticket/token 500 may be either digitally signed by the issuer (session controller 425) with a public key algorithm (*e.g.*, the known RSA algorithm) or encrypted with a symmetric key algorithm (*e.g.*, the known AES or 3DES algorithms)."

with their LinkedIn profiles without their consent or notification. ¶¶66-70. Therefore, Zoom users who subscribed to the LinkedIn Sales Navigator feature were able to view links to the publicly available LinkedIn profiles of other meeting participants without their consent or notification. ¶67. This functionality even worked to display the LinkedIn profiles of users who adopted pseudonyms in Zoom Meetings in order to remain anonymous. ¶¶70, 91. As a result, Zoom Meetings would identify certain users' real names and biographical information as reflected on LinkedIn even if those users wished to keep their actual identity private and had taken steps to ensure that they would remain anonymous by adopting a pseudonym while using Zoom Meetings. ¶¶66, 70, 91.

(d) As part of a manual update for its Mac computer application in July 2018, Zoom's software installed a secret web server on its users' Mac computers. The Zoom web server was "consciously" engineered by the Company to specifically bypass security settings on the Mac-native internet browser Safari and had a vulnerability that permitted the computer's camera to be turned on remotely without consent. *See* ¶¶35, 37. The Zoom web server also remained on users' Mac computers even after the users deleted the Zoom app. Zoom knew about or deliberately disregarded this security vulnerability. The Company was informed of the vulnerability by a software security engineer on March 26, 2019 and acknowledge that it had received that communication on April 1, 2019, before the start of the Class Period. ¶35.

C. While Zoom's Stock Price Surges, a Security Researcher Discloses a Security Vulnerability on Mac Computers

35. On July 8, 2019, software security engineer Jonathan Leitschuh ("Leitschuh") published an article on Medium's InfoSec Write-ups titled, "Zoom Zero Day: 4+ Million Webcams & maybe an RCE? Just get them to visit your website!"[9] The article disclosed vulnerabilities of using Zoom on Mac computers, which allowed malicious websites to enable a user's camera without consent. The article also disclosed Defendants' covert installation of a local web server on Mac computers, which remained on the computer even if users uninstalled Zoom. Leitschuh reported that he had communicated the security vulnerability to Zoom on March 26, 2019, which Zoom acknowledged on April 1, 2019 – prior to the start of the Class Period. Leitschuh further reported

[9] Medium is an online digital publishing platform featuring articles from independent writers.

communicating with Zoom, including its security team, regarding the vulnerability on April 18 and 19, and subsequently on June 7, 11 and 20, 2019, but that Zoom's security team did not take the vulnerabilities seriously:

> ***A vulnerability in the Mac Zoom Client allows any malicious website to enable your camera without your permission. The flaw potentially exposes up to 750,000 companies around the world that use Zoom to conduct day-to-day business***.
>
> * * *
>
> This vulnerability allows any website to forcibly join a user to a Zoom call, with their video camera activated, without the user's permission.
>
> On top of this, this vulnerability would have allowed any webpage to DOS (Denial of Service) a Mac by repeatedly joining a user to an invalid call.
>
> Additionally, if you've ever installed the Zoom client and then uninstalled it, you still have a localhost web server on your machine that will happily re-install the Zoom client for you, without requiring any user interaction on your behalf besides visiting a webpage. This re-install 'feature' continues to work to this day.
>
> * * *
>
> As of 2015 Zoom had over 40 million users. Given that Macs are 10% of the PC market and Zoom has had significant growth since 2015 we can assume that at least 4 million of Zoom's users are on Mac. . . .
>
> Any vulnerability in an application with this many users must be considered a serious threat to all those users. All of the vulnerabilities described in this report can be exploited via "drive-by attack" methodologies. Many times during my conversation with the Zoom security team they seemed to argue that the seriousness of this vulnerability was limited because it would require "user interaction" to exploit these. My response to this was finally "I would highly suggest that you not hang your hat on 'user interaction required' for protecting your users given that this 'user interaction' is simply clicking a link or visiting a webpage."

36. Following these disclosures, Zoom's stock price fell $1.12 per share from its closing price of $91.88 on July 5, 2019 to close at $90.76 on July 8, 2019.

37. On July 11, 2019, the Electronic Privacy Information Center ("EPIC") filed a complaint against Zoom with the FTC. EPIC's complaint alleged that Zoom intentionally designed its videoconferencing services to bypass browser security settings, thereby "plac[ing] at risk the privacy and security of the users of its services." Further, the complaint stated that: "When informed of the vulnerabilities Zoom did not act until the risks were made public, several months after the matter was brought to the company's attention." EPIC's complaint, based in part on Leitschuh's

findings, also detailed that remote access to Zoom users' webcams without their consent was possible, potentially subjecting users to remote surveillance, and also vulnerable to denial of service attacks.

38. EPIC's complaint also explained Defendants' admitted purpose for covertly installing the web server – to prevent Zoom users who are using the Mac-based web browser Safari from having Safari's security setting require them to click more than once to join a Zoom meeting:

> When a Mac-user installs the Zoom client, Zoom also installs a localhost web server on the device without the user's knowledge. The localhost web server allows users to join Zoom meetings without manually launching the Zoom client, but also allows others to join users to Zoom meetings without their knowledge or consent.
>
> ***Zoom developed this technique to bypass a security feature in Safari 12, which required users to affirmatively choose to join a Zoom meeting***. Zoom contends that the installation of the Zoom local web server "is a legitimate solution to a poor user experience problem, enabling our users to have faster, one-click-to-join meetings."
>
> * * *
>
> Zoom's Chief Information Security Officer Richard Farley acknowledges this design choice – "***[w]e consciously enabled the ability to have meeting joins initiated from within an iframe on a webpage***" – but claims that it is "not a security concern."

D. Defendants' July 2019 to March 2020 Materially False and Misleading Statements Regarding Encryption, Security and Data Privacy

39. Despite the disclosures in the Leitschuh article and EPIC complaint, Defendants' misrepresentations continued unabated. On July 12, 2019, Defendants published an article on Zoom's blog titled, "The Rise of Cloud Video Conferencing in Financial Services." That blog post again stated that consumers of video conferencing products required "end-to-end encryption," highlighting the importance of the security feature while implying that Zoom's platform in fact used end-to-end encryption:

> Compliance and security: ***Financial services organizations require security features like end-to-end encryption***, the ability to control access to meetings and recordings, single sign-on, and support for role-based security models.

40. On September 10, 2019, Argus Research published an analyst report that described the reputational damage to the Company stemming from Zoom's prioritization of ease of use over

user privacy and security in connection with Zoom's installation of a local web server on Mac clients, first identified in Leitschuh's July 8, 2019 article:

> Zoom got a PR black eye on July 8 when security researcher Jonathan Leitschuh publicly disclosed a security vulnerability related to the local web server installed on users' Apple computers with the Zoom application. The flaw would enable a third party to automatically turn on a user's web camera as well as enable denial of service attacks on the user's computer. While the DNS flaw was fixed in May, the web camera issue was not adequately addressed until after Mr. Leitschuh went public, after the expiration of the customary 90-day waiting period from when Mr. Leitschuh first reported the flaw privately to the company.
>
> We can see how the company's ethic around creating an easy and seamless user experience may have led to decisions to automate certain processes to save users redundant click throughs. However, issues around the tech industry's responsibility for user privacy and data security have intensified severely in recent years after Facebook's Cambridge Analytica scandal, the continuing string of large data breaches, and increased regulatory scrutiny of industry business practices. While Zoom did quickly fix the flaw after public disclosure, the company's stumble arose from not taking a flaw that could compromise user privacy seriously enough to fix it earlier.

41. At the October 15, 2019 Zoomtopia conference, in response to an analyst's question about Zoom's security features, CEO Yuan touted the Company's security capabilities, highlighting that its customers do not have a lot of questions about security of data privacy once they review the Company's security white paper, which remained on its website, and continued to state that Zoom meetings enabled end-to-end encryptions:

> [Analyst:] So as you move upstream, regardless of all the features that customers love, talk a little bit about how customers are demanding additional security features. . . .
>
> [Yuan:] Yes, yes. That's a good question. . . . I came from WebEx, right? When we build WebEx, we never realized we needed to add those security features. We distribute all the features. They come – whenever we receive a report about any [embedded] issues, we try to fix those security problems. I learned a hard lesson. That's why Zoom on day 1, security is already built in from each layer, right, with a security interface, with security interface. I think if you look at our product today, from a security feature perspective, I think we pretty much already offer a lot of security features. . . .
>
> Another thing more of the customer data privacy is very important, and customers use our cloud, recording the meetings, maybe they pay for with a credit card, we're going to make sure, show customer that those layers, what we can do to have a customer privacy. But most of the time, other customer looking at our security white paper, they do not have a lot of questions about our security features, just, I mean, data privacy and a compliance, yes, on that front.

42. The then-current version of Zoom's "security white paper" referenced by Yuan at Zoomtopia was the June 2019 Security Guide. As of October 15, 2019, the June 2019 Security Guide continued to misleadingly represent that: "Zoom places security as the highest priority in the operations of its suite of products and services." The security white paper continued to falsely state that the meeting host could enable end-to-end encryption before or during a Zoom meeting:

> The following pre-meeting security capabilities are available to the meeting host:
>
> • ***Enable an end-to-end (E2E) encrypted meeting***.
>
> * * *
>
> The following in-meeting security capabilities are available to the meeting host:
>
> • ***Secure a meeting with E2E encryption***.

43. By November 4, 2019, Zoom's website added a page at https://zoom.us/security titled, "Security at Zoom" that included a graphic falsely depicting settings available in Zoom's app for toggling "***[e]nd-to-end encryption***" on and off to "***[r]equire all meetings [be] encrypted using AES***." "Security at Zoom" further represented that Zoom takes security seriously and was committed to protecting users' privacy and falsely stated that it was protecting users by offering "end-to end encryption" for secure meetings and communications:

> We take security seriously and we are proud to exceed industry standards when it comes to your organizations communications.
>
> * * *
>
> Protecting your Privacy
>
> Zoom is committed to protecting your privacy. ***We've designed policies and controls to safeguard the collection, use, and disclosure of your information.***
>
> Protecting your Meetings
>
> The following in-meeting security capabilities are available to the meeting host:
>
> • ***Secure a meeting with end-to-end encryption***.

44. On November 22, 2019, Guggenheim issued an analyst report identifying the importance of the end-to-end encryption feature in Zoom's Video Content-as-a-Service ("VCaaS") offering and highlighted that end-to-end encryption protected "all types of [Zoom's] meetings":

> Meetings and Chat: HD audio and video brings together participants through two effective channels of communication. Meetings can be hosted as 1:1 or with multiple participants. Chat messaging functions are also available within video meetings that further broaden the scope of VCaaS capability. ***The cloud is built with end-to-end encryption to protect all types of meetings***.

45. On December 31, 2019, Zoom updated its Privacy Policy but continued to include false and misleading representations about its collection, use and disclosure of personal data:

> ***This policy outlines our data handling practices, and in particular how we collect, use, and disclose Personal Data***.
>
> * * *
>
> [W]e may ***collect*** Personal Data from or about you when you use or otherwise interact with our Products. We may gather the following categories of Personal Data about you:
>
> * * *
>
> - ***Facebook profile information (when you use Facebook to log-in to our Products or to create an account for our Products)***

46. On February 23, 2020 and March 18, 2020, Zoom updated its Privacy Policy but continued to include false and misleading representations about its collection, use and disclosure of personal data:

> ***This policy outlines our data handling practices, and in particular how we collect, use, and disclose Personal Data***. It covers all Personal Data that you affirmatively provide during your interactions with us, information that we automatically collect when you interact with our Products, and information that we collect about you from third parties.
>
> * * *
>
> Whether you have Zoom account or not, we may ***collect*** Personal Data from or about you when you use or otherwise interact with our Products. We may gather the following categories of Personal Data about you:
>
> * * *
>
> - ***Facebook profile information (when you use Facebook to log-in to our Products or to create an account for our Products)***

E. Reasons Defendants' July 2019 to March 2020 Material Misrepresentations Regarding Encryption, Security and Privacy Were Made Knowingly or with Deliberate Recklessness

47. Each of Defendants' statements in ¶¶39, 41-43 and 45-46 concerning Zoom's purportedly robust security capabilities, including the availability of end-to-end AES 256-bit

encryption and the scope of the collection and use of personal data as represented in its Privacy Policy, was materially false and misleading when made, as Defendants knew or deliberately disregarded and failed to disclose the following facts:

(a) Zoom Meetings were ***not*** in fact secured with end-to-end encryption. Instead, Zoom maintained access to the cryptographic keys for Zoom Meetings such that the Company could decrypt and decipher the communications between end users. Whereas end-to-end encryption means that not even the company that runs the messaging service can access the cryptographic keys necessary to decrypt the end users' communications, here Zoom maintained access to the cryptographic keys that could allow Zoom to decrypt and decipher the communications between the end users, thereby breaking the "end-to-end promise." Zoom's server was therefore not an illiterate messenger, and Zoom could decipher the messages that it passed between users. Defendants knew the meaning of end-to-end encryption; and, in fact, they used the term accurately in other contexts, including in describing Zoom's end-to-end chat encryption in the Company's security white papers. ¶34(a) n.6. Further, Yuan himself led the effort to engineer Zoom Meetings' platform and is named on several patents that specifically concern encryption techniques. Nor did Zoom use AES 256-bit encryption to secure the content of communications between users of Zoom Meetings. In truth, Zoom used AES 128-bit encryption, a lower level of encryption to encrypt and decrypt audio and video in Zoom Meetings. AES 128-bit encryption provides less secure protection of users' communications than AES 256-bit encryption.

(b) While Zoom's Privacy Policy disclosed that the Company may ***collect*** users' personal data "when [users] use Facebook to log-in to our Products or to create an account for our Products," it failed to disclose that Zoom was surreptitiously sending users' data to Facebook – including from users who did not have a Facebook account – without their consent or notification. Notably, Facebook required that developers that use its SDK, such as Zoom, be transparent with users about the data their apps send to Facebook. ¶49.

(c) When users signed into a meeting, Zoom's software automatically and surreptitiously sent their names and e-mail addresses to a company system it used to match them with their LinkedIn profiles without their consent or notification. ¶¶66-70. Therefore, Zoom users

who subscribed to the LinkedIn Sales Navigator feature were able to view links to the publicly available LinkedIn profiles of other meeting participants without their consent or notification. ¶67. This functionality even worked to display the LinkedIn profiles of users who adopted pseudonyms in Zoom Meetings in order to remain anonymous. ¶¶70, 91. As a result, Zoom Meetings would identify certain users' real names and biographical information as reflected on LinkedIn even if those users wished to keep their actual identity private and had taken steps to ensure that they would remain anonymous by adopting a pseudonym while using Zoom Meetings. ¶66, 70, 91.

VII. THE TRUTH BEGINS TO BE REVEALED

A. The Website Motherboard Reports that Zoom Sends User Data to Facebook, Including from Non-Facebook Users

48. On March 26, 2020, the website Motherboard published an article titled, "Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account: Zoom's privacy policy isn't explicit about the data transfer to Facebook at all." The article revealed that the Company was sending data to Facebook, including from users without Facebook accounts, and noted there was "nothing in the privacy policy that addresses" that, by using Zoom, users may be providing data to Facebook:

> As people work and socialize from home, video conferencing software Zoom has exploded in popularity. ***What the company and its privacy policy don't make clear is that the iOS version of the Zoom app is sending some analytics data to Facebook, even if Zoom users don't have a Facebook account***, according to a Motherboard analysis of the app.
>
> This sort of data transfer is not uncommon, especially for Facebook; plenty of apps use Facebook's software development kits (SDK) as a means to implement features into their apps more easily, which also has the effect of sending information to Facebook. But Zoom users may not be aware it is happening, nor understand that when they use one product, they may be providing data to another service altogether.
>
> "***That's shocking. There is nothing in the privacy policy that addresses that***," Pat Walshe, an activist from Privacy Matters who has analyzed Zoom's privacy policy, said in a Twitter direct message.

49. The Motherboard article analyzed Zoom's Privacy Policy, which did ***not*** disclose that Defendants would send data about Zoom users who do not even have a Facebook account to Facebook, and quoted Facebook's terms of use, which required Defendants to "provide[] robust and sufficiently prominent notice to users regarding the Customer Data collection, sharing and usage,"

thereby indicating that Defendants acted with knowledge or deliberate recklessness in failing to disclose that Zoom users' data was being sent to Facebook even if they did not have a Facebook account:

> Zoom is not forthcoming with the data collection or the transfer of it to Facebook. Zoom's policy says the company may ***collect*** user's "Facebook profile information (when you use Facebook to log-in to our Products or to create an account for our Products)," but doesn't explicitly mention anything about ***sending data to Facebook*** on Zoom users ***who don't have a Facebook account at all***.
>
> Facebook told Motherboard it requires developers to be transparent with users about the data their apps send to Facebook. Facebook's terms say "If you use our pixels or SDKs, you further represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Customer Data collection, sharing and usage," and specifically for apps, "that third parties, including Facebook, may collect or receive information from your app and other apps and use that information to provide measurement services and targeted ads."

50. On March 27, 2020, CEO Yuan wrote a blog post published on Zoom's blog addressing the Motherboard article, in which Yuan admitted that Defendants collected "unnecessary" user information by using Facebook's SDK:

> Zoom takes its users' privacy extremely seriously. We would like to share a change that we have made regarding the use of Facebook's SDK.
>
> We originally implemented the "Login with Facebook" feature using the Facebook SDK for iOS (Software Development Kit) in order to provide our users with another convenient way to access our platform. However, we were made aware on Wednesday, March 25, 2020, that the Facebook SDK was collecting device information unnecessary for us to provide our services. The information collected by the Facebook SDK did not include information and activities related to meetings such as attendees, names, notes, etc., but rather included information about devices such as the mobile OS type and version, the device time zone, device OS, device model and carrier, screen size, processor cores, and disk space.
>
> Our customers' privacy is incredibly important to us, and therefore we decided to remove the Facebook SDK in our iOS client and have reconfigured the feature so that users will still be able to log in with Facebook via their browser.

51. On March 29, 2020, Zoom updated its Privacy Policy. The Privacy Policy included a letter from Aparna Bawa, Zoom's Chief Legal Officer, that reiterated the importance of users' privacy to the Company: "Privacy is an extremely important topic, and we want you to know that at Zoom, we take it very seriously. . . . We are committed to protecting the privacy and security of your personal data."

B. *The New York Times* Reports that the New York Attorney General Is Investigating Zoom's Data Privacy and Security Practices

52. On March 30, 2020, *The New York Times* published an article titled, "New York Attorney General Looks Into Zoom's Privacy Practices: As the videoconferencing platform's popularity has surged, Zoom has scrambled to address a series of data privacy and security problems." The article reported that Zoom was being investigated by the New York Attorney General for its security and privacy practices, including data sharing with Facebook and security vulnerabilities that allowed malicious websites to enable a user's webcam without consent. The New York Attorney General was said to have sought information on "'the categories of data that Zoom collects, as well as the purposes and entities to whom Zoom provides consumer data,'" and on "changes the company put in place after a security researcher, Jonathan Leitschuh, exposed a flaw allowing hackers to take over Zoom webcams." The article also reported on the Motherboard article disclosing that Zoom was sending users' data to Facebook. The article stated:

> Zoom, the videoconferencing app whose traffic has surged during the coronavirus pandemic, is under scrutiny by the office of New York's attorney general, Letitia James, for its data privacy and security practices.
>
> On Monday, the office sent Zoom a letter asking what, if any, new security measures the company has put in place to handle increased traffic on its network and to detect hackers, according to a copy reviewed by The New York Times.
>
> While the letter referred to Zoom as "an essential and valuable communications platform," it outlined several concerns, noting that the company had been slow to address security flaws such as vulnerabilities "that could enable malicious third parties to, among other things, gain surreptitious access to consumer webcams."
>
> * * *
>
> As Zoom's popularity has grown, the app has scrambled to address a series of data privacy and security problems, a reactive approach that has led to complaints from some consumer, privacy and children's groups.

53. On March 30, 2020, Zoom's stock price opened at $160.76 and declined to a low of $147.20 before closing at $150.88 per share. On March 31, 2020, Zoom's stock price declined from a close of $150.88 on March 30, 2020 to a low of $143.36 per share before closing at $146.12.

54. On March 31, 2020, Benzinga published an article titled, "Zoom Shares Drop As New York Attorney General Looks Into Company's Privacy, Security Practices" that reported Zoom's stock was declining in response to the New York Attorney General's investigation:

> The shares of Zoom Video Communications (NASDAQ: ZM) dropped 6.14% lower at Monday's close compared to the day's open at $160.76.
>
> * * *
>
> The drop came as the New York Times reported that the office of the New York Attorney General is probing the company's data privacy and security practices.
>
> * * *
>
> Citing a report by Motherboard last week that said that Zoom shared customer data with Facebook Inc. (NASDAQ: FB) without explicit consent, James' office asked for "the categories of data that Zoom collects, as well as the purposes and entities to whom Zoom provides consumer data."

55. Also on March 31, 2020, TheStreet.com referenced *The New York Times* article and reported that Zoom was under scrutiny in an article titled, "Zoom Video Under Scrutiny for Data Privacy and Security Practices." The article stated that "[s]hares of Zoom Video were down 3.07% at $146.25 in morning trading on Tuesday."

C. *The Intercept* Reports – and Defendants Admit – that Zoom Meetings Are *Not* End-to-End Encrypted

56. On March 31, 2020, before the market opened, computer security engineer Micah Lee and journalist Yael Grauer published an article on *The Intercept* titled, "ZOOM MEETINGS AREN'T END-TO-END ENCRYPTED, DESPITE MISLEADING MARKETING: The video conferencing service can access conversations on its platform." The article disclosed that Defendants' claim that Zoom users could enable end-to-end encryption was false. The Company's Zoom Meetings did ***not*** provide end-to-end encryption. Instead, the Company used a weaker form of encryption called "transport encryption," which provided not just the users but also Zoom itself the decryption key. Indeed, the article quoted Defendants as admitting that: "'***Currently, it is not possible to enable E2E [end-to-end] encryption for Zoom video meetings***,'" despite having repeatedly represented that it was not only possible but a present option for users. The article called Defendants' end-to-end encryption representations "misleading marketing."

> Zoom, the video conferencing service whose use has spiked amid the Covid-19 pandemic, ***claims to implement end-to-end encryption, widely understood as the most private form of internet communication, protecting conversations from all outside parties. In fact, Zoom is using its own definition of the term, one that lets Zoom itself access unencrypted video and audio from meetings***.
>
> * * *
>
> Still, Zoom offers reliability, ease of use, and at least one very important security assurance: As long as you make sure everyone in a Zoom meeting connects using "computer audio" instead of calling in on a phone, the meeting is secured with end-to-end encryption, at least according to Zoom's website, its security white paper, and the user interface within the app. But ***despite this misleading marketing, the service actually does not support end-to-end encryption for video and audio content, at least as the term is commonly understood***. Instead it offers what is usually called transport encryption, explained further below.
>
> * * *
>
> In Zoom's white paper, there is a list of "pre-meeting security capabilities" that are available to the meeting host that starts with "Enable an end-to-end (E2E) encrypted meeting." Later in the white paper, it lists "Secure a meeting with E2E encryption" as an "in-meeting security capability" that's available to meeting hosts. When a host starts a meeting with the "Require Encryption for 3rd Party Endpoints" setting enabled, participants see a green padlock that says, "Zoom is using an end to end encrypted connection" when they mouse over it.
>
> But when reached for comment about whether video meetings are actually end-to-end encrypted, ***a Zoom spokesperson wrote, "Currently, it is not possible to enable E2E encryption for Zoom video meetings***. Zoom video meetings use a combination of TCP and UDP. TCP connections are made using TLS and UDP connections are encrypted with AES using a key negotiated over a TLS connection."

57. *The Intercept* article further explained that because Zoom had the ability to decrypt communications, Zoom Meetings did not in fact offer end-to-end encryption:

> The encryption that Zoom uses to protect meetings is TLS, the same technology that web servers use to secure HTTPS websites. . . . This is known as transport encryption, which is different from end-to-end encryption because the Zoom service itself can access the unencrypted video and audio content of Zoom meetings. So when you have a Zoom meeting, the video and audio content will stay private from anyone spying on your Wi-Fi, but it won't stay private from the company. . . .
>
> For a Zoom meeting to be end-to-end encrypted, the video and audio content would need to be encrypted in such a way that only the participants in the meeting have the ability to decrypt it. The Zoom service itself might have access to encrypted meeting content, but wouldn't have the encryption keys required to decrypt it (only meeting participants would have these keys) and therefore, would not have the technical ability to listen in on your private meetings. This is how end-to-end encryption in messaging apps like Signal work: The Signal service facilitates sending encrypted messages between users, but doesn't have the encryption keys required to decrypt those messages and therefore, can't access their unencrypted content.

> "When we use the phrase 'End to End' in our other literature, it is in reference to the connection being encrypted from Zoom end point to Zoom end point," the Zoom spokesperson wrote, apparently referring to Zoom servers as "end points" even though they sit between Zoom clients. "The content is not decrypted as it transfers across the Zoom cloud" through the networking between these machines.

58. *The Intercept* article also reported that Matthew Green, a computer science professor at Johns Hopkins, said that end-to-end encryption of videoconferencing is possible and offered by other videoconferencing products such as Apple's FaceTime. Green called Zoom's representations that end-to-end encryption was available on its platform "slightly dishonest" and said he wished "they just came clean":

> "If it's all end-to-end encrypted, you need to add some extra mechanisms to make sure you can do that kind of 'who's talking' switch, and you can do it in a way that doesn't leak a lot of information. You have to push that logic out to the endpoints," he told The Intercept. This isn't impossible, though, Green said, as demonstrated by Apple's FaceTime, which allows group video conferencing that's end-to-end encrypted. "It's doable. It's just not easy."
>
> "They're a little bit fuzzy about what's end-to-end encrypted," Green said of Zoom. "***I think they're doing this in a slightly dishonest way. It would be nice if they just came clean***."

59. Additionally, *The Intercept* article quoted the FTC's former chief technologist, who stated that if Zoom claimed to provide end-to-end encryption (as it had), those representations could be a deceptive trade practice that harms consumers and competitors that do not misrepresent their product's capabilities:

> Independent technologist Ashkan Soltani, who formerly served as the FTC's chief technologist, said it's unclear to him whether Zoom is actually implementing end-to-end encryption; he was unaware that it claimed to do so prior to speaking with The Intercept. But he said that if a reasonable consumer makes a decision to use Zoom with the understanding that it has end-to-end encryption for video chat when, in fact, it did not, and if Zoom's representation is deceptive, it could be a deceptive trade practice.
>
> This kind of marketing could impact not just consumers, but also other businesses.
>
> "***If Zoom claimed they have end-to-end encryption, but didn't actually invest the resources to implement it***, and Google Hangouts didn't make that claim and you chose Zoom, not only are you being harmed as consumer, but in fact, Hangouts is being harmed because ***Zoom is making claims about its product that are not true***," he said. "So it's actually benefiting from false claims, and people are essentially receiving more market share because of those false claims."

60. *The Intercept* article concluded with a statement provided by Defendants that stated Zoom collected data from individuals only as needed to provide effective services:

> Zoom provided the following statement to The Intercept: "Zoom takes its users' privacy extremely seriously. Zoom only collects data from individuals using the Zoom platform as needed to provide the service and ensure it is delivered as effectively as possible. Zoom must collect basic technical information like users' IP address, OS details and device details in order for the service to function properly. Zoom has layered safeguards in place to protect our users' privacy, which includes preventing anyone, including Zoom employees, from directly accessing any data that users share during meetings, including – but not limited to – the video, audio and chat content of those meetings. Importantly, Zoom does not mine user data or sell user data of any kind to anyone."

61. On March 31, 2020, Zoom's stock price declined from the prior day's close of $150.88 to a low of $143.36 per share during intraday trading before closing at $146.12. On April 1, 2020, Zoom's stock continued to decline from as low as $135.18 before closing at $137.00.

62. On April 1, 2020, after market close, Yuan published "A Message to Our Users" on Zoom's blog. Yuan admitted that Zoom had "fallen short" of meeting the Company's and its users "privacy and security expectations," said the Company removed the software that shared Zoom user data with Facebook and "clarif[ied] the facts" about the ability to encrypt transmissions over Zoom's platform:

> For the past several weeks, supporting this influx of users has been a tremendous undertaking and our sole focus. We have strived to provide you with uninterrupted service and the same user-friendly experience that has made Zoom the video-conferencing platform of choice for enterprises around the world, while also ensuring platform safety, privacy, and security. However, ***we recognize that we have fallen short of the community's – and our own – privacy and security expectations***. For that, I am deeply sorry, and I want to share what we are doing about it.
>
> * * *
>
> • ***On March 27th, we took action to remove the Facebook SDK in our iOS client*** and have reconfigured it to prevent it from collecting unnecessary device information from our users.
>
> * * *
>
> • ***On April 1, we:***
>
> ◦ ***Published a blog to clarify the facts around encryption on our platform – acknowledging and apologizing for the confusion***.

63. Yuan's April 1, 2020 blog post referred and linked to a post of the same date by Oded Gal ("Gal"), Zoom's Chief Product Officer, titled, "The Facts Around Zoom and Encryption for

Meetings/Webinars."[10] Therein, Defendants admitted that Zoom meetings were ***not*** capable of using end-to-end encryption and apologized for "incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption." The Company also admitted that its use of the term "end-to-end encryption" conflicted with the commonly-accepted definition of the term:

> In light of recent interest in our encryption practices, we want to start by ***apologizing for the confusion we have caused by incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption***. Zoom has always strived to use encryption to protect content in as many scenarios as possible, and in that spirit, we used the term end-to-end encryption. While we never intended to deceive any of our customers, ***we recognize that there is a discrepancy between the commonly accepted definition of end-to-end encryption and how we were using it***. This blog is intended to rectify that discrepancy and clarify exactly how we encrypt the content that moves across our network.

64. On April 2, 2020, CNBC published an article titled, "Zoom falls 11% after CEO apologizes for security lapses, says daily users spiked to 200 million in March," which reported on Yuan's apology for security lapses and noted that "shares of Zoom cratered." The article stated:

> Zoom CEO Eric Yuan apologized on Thursday for security lapses that have been reported this week and outlined what the company is doing to fix those problems.
>
> He also said the company saw a huge spike in users, up to 200 million people per day in March, from about 10 million in December.
>
> Zoom closed at $121.93 per share, down 11% on the day. Shares of Zoom were down as much as 16% on Thursday morning.

65. On April 2, 2020, Zoom's stock price declined further from the prior day's closing price of $137.00 to a low of $114.50 during intraday trading before closing at $121.93 per share.

D. *The New York Times* Reports that Zoom Secretly Displayed Data from Users' LinkedIn Accounts

66. After market close on April 2, 2020, *The New York Times* published an article titled, "A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles: After an inquiry from Times reporters, Zoom said it would disable a data-mining feature that could be used to snoop on participants during meetings without their knowledge." The article detailed numerous security

[10] Yuan recruited Gal, a former WebEx colleague, and as of April 19, 2019 they shared an office with each other at Zoom.

and privacy concerns related to the fact that Zoom permitted certain users to access other users' LinkedIn profile information without their knowledge:

> ***[W]hat many people may not know is that, until Thursday, a data-mining feature on Zoom allowed some participants to surreptitiously have access to LinkedIn profile data about other users – without Zoom asking for their permission during the meeting or even notifying them that someone else was snooping on them***.
>
> The undisclosed data mining adds to growing concerns about Zoom's business practices at a moment when public schools, health providers, employers, fitness trainers, prime ministers and queer dance parties are embracing the platform.
>
> An analysis by The New York Times found that when people signed in to a meeting, Zoom's software automatically sent their names and email addresses to a company system it used to match them with their LinkedIn profiles.
>
> * * *
>
> The discoveries about Zoom's data-mining feature echo what users have learned about the surveillance practices of other popular tech platforms over the last few years. The video-meeting platform that has offered a welcome window on American resiliency during the coronavirus – providing a virtual peek into colleagues' living rooms, classmates' kitchens and friends' birthday celebrations – can reveal more about its users than they may realize.
>
> "People don't know this is happening, and that's just completely unfair and deceptive," Josh Golin, the executive director of the Campaign for a Commercial-Free Childhood, a nonprofit group in Boston, said of the data-mining feature.

67. The April 2, 2020 article in *The New York Times* noted that after reporters contacted Zoom with their findings, the Company disabled the data-mining feature as follows:

> Early Thursday, after Times reporters contacted Zoom and LinkedIn with their findings on the profile-matching feature, the companies said they would disable the service.
>
> In a statement, Zoom said it took users' privacy "extremely seriously" and was "removing the LinkedIn Sales Navigator to disable the feature on our platform entirely." In a related blog post, Eric S. Yuan, the chief executive of Zoom, wrote that the company had removed the data-mining feature "after identifying unnecessary data disclosure." He also said Zoom would freeze all new features for the next 90 days to concentrate on data security and privacy issues.

68. The April 2, 2020 article in *The New York Times* provided the following details about Zoom's promotion of the LinkedIn profile-matching feature the Company introduced in 2018:

> In 2018, Zoom introduced the LinkedIn profile-matching feature to help sales representatives better profile and target sales prospects attending Zoom meetings.
>
> "Instantly gain insights about your meeting participants," a Zoom video promoting the service said. "Once signed in, you'll be able to match participants to their LinkedIn profile information and view their recent activity."

69. The April 2, 2020 article also summarized Zoom's privacy shortcomings, placing the latest issue regarding LinkedIn in the larger context of privacy and security issues and demonstrating that Defendants had prioritized growth at the expense of privacy and security:

> Privacy experts said the company seemed to value ease of use and fast growth over instituting default user protections.
>
> "It's a combination of sloppy engineering and prioritizing growth," said Jonathan Mayer, an assistant professor of computer science and public affairs at Princeton University. "It's very clear that they have not prioritized privacy and security in the way they should have, which is obviously more than a little concerning."
>
> In response to news reports on its problems, Zoom recently announced that it had stopped using software in its iPhone app that sent users' data to Facebook; updated its privacy policy to clarify how it handles user data; and conceded that it had overstated the kind of encryption it used for video and phone meetings.
>
> Although profiling consumers and prospecting for corporate clients are standard practices in sales and customer relations management, privacy experts criticized Zoom for making the data-mining tools available during meetings without alerting participants as they were being subjected to them.

70. The April 2, 2020 article also detailed that Defendants' Privacy Policy and terms of service failed to disclose that the data-mining feature could be used to reveal LinkedIn data of participants during meetings without their knowledge:

> But neither Zoom's privacy policy nor its terms of service specifically disclosed that Zoom could covertly display meeting participants' LinkedIn data to other users – or that it might communicate the names and email addresses of participants in private Zoom meetings to LinkedIn. In fact, user instructions on Zoom suggested just the opposite: that meeting attendees may control who sees their real names.
>
> "Enter the meeting ID number and your display name," one section on Zoom's Help Center said. "If you're signed in, change your name if you don't want your default name to appear."
>
> Similarly, Zoom's privacy policy says that "some data will be disclosed to other participants" when a person uses Zoom. For instance, it says, "if you send a chat or share content, that can be viewed by others in the chat or the meeting." But it did not mention that Zoom could show some users' LinkedIn data to other users or disclose data about users' participation in private Zoom meetings to LinkedIn.

E. University of Toronto's Citizen Lab Reports that Zoom's Encryption Has Significant Weaknesses

71. On April 3, 2020 during intraday trading hours, Citizen Lab, an interdisciplinary laboratory at the Munk School of Global Affairs, University of Toronto, issued a report titled,

"Move Fast and Roll Your Own Crypto A Quick Look at the Confidentiality of Zoom Meetings." The report said "that the Zoom app uses non-industry-standard cryptographic techniques with identifiable weaknesses." The report also stated that, contrary to Zoom's representations that it uses AES 256-bit encryption, the Company in fact uses AES 128-bit encryption, that the Zoom servers that generate the AES 128-bit keys are at times located in China even where all participants in a Zoom meeting are outside of China and that, as a result, Zoom may be subject to pressure from Chinese authorities:

> • Zoom documentation claims that the app uses "AES-256" encryption for meetings where possible. However, we find that in each Zoom meeting, a single AES-128 key is used in ECB mode by all participants to encrypt and decrypt audio and video. The use of ECB mode is not recommended because patterns present in the plaintext are preserved during encryption.
>
> • The AES-128 keys, which we verified are sufficient to decrypt Zoom packets intercepted in Internet traffic, appear to be generated by Zoom servers, and in some cases, are delivered to participants in a Zoom meeting through servers in China, even when all meeting participants, and the Zoom subscriber's company, are outside of China.
>
> • . . . However, this arrangement may make Zoom responsive to pressure from Chinese authorities.[11]

72. Citizen Lab's report also confirmed that Zoom did not use "end-to-end encryption":

> Zoom's documentation has a number of unclear claims about encryption that the platform offers. Some Zoom documentation (as well as the Zoom app itself) claims that Zoom offers a feature for "end-to-end (E2E) encrypted meetings.
>
> Typically, the computer security community understands the term "end-to-end encrypted" to mean that only the parties to the communication can access it (and not any middlemen that relay the communication).
>
> * * *
>
> In response to this confusion, Zoom released a blog post in April 2020 describing their encryption scheme. The blog post clarifies that Zoom does not currently implement "end-to-end" encryption as most people understand the term; Zoom used the term "end-to-end" to describe a situation where all conference participants (except those dialing in via the public switched telephone network) are required to use transport encryption between their devices and Zoom servers. Zoom's definition of "end-to-end" does not seem to be a standard one, even in the realm of enterprise videoconferencing solutions. Because Zoom does not implement true end-to-end encryption, they have the theoretical ability to decrypt and monitor Zoom calls.

[11] Indeed, on December 18, 2020, the DOJ indicted a former Zoom executive for participating in a scheme to disrupt a series of meetings held to commemorate the 1989 Tiananmen Square massacre.

73. Multiple news organizations covered Citizen Lab's April 3, 2020 report, including the BBC in an April 3, 2020 article titled, "Zoom 'unsuitable' for government secrets, researchers say," and *Forbes* in an April 3, 2020 article titled, "Warning: Zoom Makes Encryption Keys In China (Sometimes)."

74. On April 3, 2020, Defendants published "Response to Research From University of Toronto's Citizen Lab" by CEO Yuan on Zoom's blog, where he acknowledged that the Company needed to improve with respect to encryption, stating in relevant part: "We recognize that we can do better with our encryption design."

75. On the same day, *The Wall Street Journal* published an article titled, "Zoom CEO: 'I Really Messed Up' on Security as Coronavirus Drove Video Tool's Appeal: Eric Yuan says he is scrambling to restore reputation of platform that has drawn soaring usage, privacy concerns during pandemic." *The Wall Street Journal* article was based on an interview conducted with Yuan, in which he stated that he was now promising a future option for end-to-end encryption in a few months. It also noted that large companies such as Tesla had stopped using the Zoom platform as a result of the Company's security failings.

> "'If we mess up again, it's done,' I thought a lot last night," he told The Wall Street Journal in an interview Friday, after what he said was a sleepless night.
>
> Among the privacy features Mr. Yuan now promises is an option for end-to-end encryption to safeguard conversations, he told the Journal. Zoom had previously advertised such a feature, but security experts discovered the underlying technology provided a lesser level of data protection. The full-encryption feature won't be ready for a few months, Mr. Yuan said.
>
> * * *
>
> The backlash against Zoom hasn't come just from security professions. Some corporate users have dropped the platform, including Elon Musk's Tesla Inc. and Space Exploration Technologies Corp., Mr. Yuan said.
>
> "I really messed up as CEO, and we need to win their trust back. This kind of thing shouldn't have happened," he said.

76. On April 6, 2020, analysts at Credit Suisse issued an analyst report noting Tesla's decision to stop using Zoom's platform, stating that "some high profile customers [had] curtail[ed] Zoom usage" and that the analysts "expect others [to] follow."

> **Security**: Zoom's exponential growth in usage has resulted in additional scrutiny of its technology, leading to a recent spike in security concerns. While many of these issues, especially those stemming from user error, will likely be resolved in short order, we anticipate others may linger for some time. Encryption concerns have already caused some high profile customers to curtail Zoom usage (demonstrating low switching costs for VC), and we expect others could follow though the majority of organizations likely have no issue.

77. Also on April 6, 2020, *Fortune* published an article title, "Zoom stock down after schools and businesses banned the meeting app over 'Zoom bombing' security issues," which reported that the Company's stock price had declined by 14.5% from security concerns, leading organizations to ban or discourage the platform's use:

> Zoom stock dropped as much as 14.5% this morning, after concerns over the security of the company's video-chat and meeting software led to several major organizations banning or discouraging its use. The reversal follows a huge surge in usage during a worldwide lockdown to combat the coronavirus pandemic.
>
> * * *
>
> Recent days have highlighted a number of deeper concerns with the underlying security of Zoom software and the company's practices. Zoom is facing lawsuits in New York and California for sharing user data with Facebook, a practice Zoom has since halted.
>
> On Friday, it was revealed that some Zoom calls were routed through data centers in China, potentially making them easier to compromise. Recent reports also found that while Zoom claimed it used "end to end encryption" to protect calls, that claim was misleading.

78. Zoom's stock price declined from a close of $128.20 on Friday, April 3, 2020 to a low of $108.53 during intraday trading on Monday, April 6, 2020 before closing at $122.94.

F. Zoom Scrubs Its Website of References to End-to-End Encryption

79. On April 6, 2020, Defendants scrubbed a number of blog posts published and maintained on Zoom's blog by removing references to "end-to-end" encryption. For example, on or around April 6, 2020, Zoom modified its July 20, 2017 blog post titled, "Zoom Feature Spotlight: Linux Client" "with an updated encryption reference" by deleting the phrase "end-to-end" from encryption from the original post. The difference between the July 20, 2017 blog post and April 6, 2020 modification is the removal of the emphasized text below:

- July 20, 2017 blog post: "Let's look at some key features of the Zoom Linux platform: . . . [e]nterprise-grade security with AES-256 bit ***end-to-end*** encryption."

- April 6, 2020 modification: "Let's look at some key features of the Zoom Linux platform: . . . [e]nterprise-grade security with AES-256 bit encryption."

80. Similarly, Zoom also modified its January 4, 2018 blog post titled, "Zoom Partners with OpenExchange to Provide Video Communications for Financial Services Market" with an updated encryption reference by removing the phrase "end-to-end" from the original post. The difference between the July 4, 2018 blog post and April 6, 2020 modification is the deletion of the emphasized text below:

- January 4, 2018 blog post: "The partnership of our video services offers numerous benefits to customers, including: . . . [s]ecure cloud (and optional hybrid cloud-onprem) communications environment with AES-256 bit ***end-to-end*** encryption."

- April 6, 2020 modification: "The partnership of our video services offers numerous benefits to customers, including: . . . [s]ecure cloud (and optional hybrid cloud/on-prem) communications environment with AES-256 bit encryption."

81. Zoom also modified its July 12, 2019 blog post titled, "The Rise of Cloud Video Conferencing in Financial Services" with an updated encryption reference by deleting the phrase "end-to-end" from the original post. The difference between the July 12, 2019 blog post and April 6, 2020 modification is the deletion of the bolded text and addition of the emphasized text below:

- July 12, 2019 blog post: "Compliance and security: Financial services organizations require security features like ***end-to-end*** encryption, the ability to control access to meetings and recordings, single sign-on, and support for role-based security models. Buyers will typically look for security certifications, including SOC 2 Type 2."

- April 6, 2020 modification: "Compliance and security: Financial services organizations require security features like encryption ***in transit***, the ability to control access to meetings and recordings, single sign-on, and support for role-based security models. Buyers will typically look for security certifications, including SOC 2 Type 2."

82. On April 7, 2020, Zoom continued to modify numerous blog posts published on its blog at blog.zoom.us "with an updated encryption reference" by deleting "end-to-end" from references to encryption:

(a) Zoom modified its January 24, 2017 blog post titled, "Zoom: The Fastest Growing App on Okta" by deleting "end-to-end":

- January 24, 2017 blog post: "Why has Zoom rocketed up the Okta's charts? The report doesn't give details, but based on feedback from our own enterprise users, we

can highlight the following features as important to businesses: . . . [s]ecure with ***end-to-end AES 256 bit encryption***."

- April 7, 2020 modification: "Why has Zoom rocketed up the Okta's charts? The report doesn't give details, but based on feedback from our own enterprise users, we can highlight the following features as important to businesses: . . . [s]ecure with AES-256 encryption."

(b) Zoom modified its April 20, 2017 blog post titled, "Introducing Zoom for Telehealth and its April 24, 2017 blog post titled, Zoom Reporting Live from American Telemedicine Association 2017," both of which contained substantially similar representations concerning encryption, by deleting "End-to-end":

- April 20 & 24, 2017 blog post: "Zoom for Telehealth includes the following features pre-configured: . . . ***[e]nd-to-end AES-256 bit encryption*** of all meeting data and instant messages."

- April 7, 2020 modification: "Zoom for Telehealth includes the following features pre-configured: . . . AES-256 bit encryption of all meeting data and instant messages."

(c) Zoom modified its February 27, 2019 blog post titled, "End-to-End Encrypted Zoom Allows FINRA to Maintain a High-Security Posture" by deleting "End-to-End Encrypted" from the title such that the title now reads, "Zoom Allows FINRA to Maintain a High-Security Posture."

(d) Zoom modified its March 30, 2020 blog post titled, "Using Zoom for Telehealth & Virtual Care" by deleting references to "end-to-end" encryption:

- March 30, 2020 blog post: "Here's what to look for in a quality video communications platform so that it adequately supports your virtual healthcare needs: . . . [c]omprehensive compliance and security protections ensure that users and administrators feel safe using a solution. A video-based telehealth solution must enable HIPAA compliance through ***end-to-end 256-bit AES encryption*** for data in transit and at rest, and without accessing protected health information."

- April 7, 2020 modification: "Here's what to look for in a quality video communications platform so that it adequately supports your virtual healthcare needs: . . . [c]omprehensive compliance and security protections ensure that users and administrators feel safe using a solution. A video-based telehealth solution must enable HIPAA compliance through 256-bit AES encryption for data in transit and at rest, and without accessing protected health information."

83. Zoom's stock price declined from a close of $122.94 on April 6, 2020 to a low of $109.57 during intraday trading on April 7, 2020 before closing at $113.75.

84. On April 8, 2020, Argus Research issued an analyst report chronicling Zoom's numerous security and privacy vulnerabilities. It discussed the vulnerability first disclosed by Leitschuh, whereby a local web server installed on users' Apple computers enabled a third party to automatically turn on the user's camera and, separately, enable denial-of-service attacks on the computer. It criticized Zoom's "fail[ure] to alert users that" their data, including data that could be used to target specific advertising at the user based on the data, was being transferred to Facebook. And it called the Company's false representation about end-to-end encryption "one more black eye for Zoom." The article concluded by noting that, as the result of these issues, 27 U.S. state attorneys general had commenced investigations into the Company.

> Another issue pointed to by the press is the company's touted 'end-to-end encryption' of its meetings software. This issue may be somewhat semantic, but it also points to a certain sloppiness by management. End-to-end encryption as generally used in the technology industry means that data is encrypted at the point of origin and then unencrypted at the endpoint such that no other parties have access to the data other than the sender and recipient, including the communication service itself. End-to-end encryption has become more common for messaging services, with the most prominent example being Facebook's WhatsApp Messenger. While Zoom said its meetings were end-to-end encrypted, its service actually has only standard encryption, which prevents outside parties from accessing the meeting but still gives Zoom itself access, which may actually be required for the software to function. So, one more black eye for Zoom. On April 1, the company clarified the type of encryption it uses. Mr. Yuan has also promised to implement real end-to-end encryption within a few months.
>
> * * *
>
> We can see how the company's interest in creating an easy user experience may have led it to automate certain processes to save users redundant click-throughs. However, concerns about tech companies' responsibility for user privacy and data security have intensified in the wake of the Facebook Cambridge Analytica scandal, the continuing string of large data breaches, and increased regulatory scrutiny of industry business practices. While Zoom quickly fixed the flaw after public disclosure, the company stumbled by not taking the threat to user privacy seriously enough and by failing to address the problem earlier.

85. Also on April 8, 2020, Oppenheimer issued an analyst report that described the negative impact from Zoom's security and privacy vulnerabilities to the Company's brand and loss of enterprise customers, triggering regulatory scrutiny of the Company.

> Zoom's recent explosive user expansion has brought new attention and high-profile criticism of its security/privacy vulnerabilities, which we believe leaves it susceptible to some brand erosion and enterprise churn. . . . Given Zoom's premium valuation (27.7x CY21 EV/sales), we remain on the sidelines, especially considering the new set of complexities Zoom's navigating.
>
> KEY POINTS
>
> • Growing pains. Zoom's seen explosive adoption from December to March, with free/paid users exponentially rising from 10M to 200M DAUs. This is indicative of Zoom's rising WFH value proposition and simple UI/user onboarding, yet it's also exposed security/privacy vulnerabilities including unobtrusive data sharing/mining, sub-standard end-to-end encryption, malicious actors accessing webcams, and exposed meeting records, which leave it vulnerable to brand erosion.
>
> * * *
>
> • Under investigation? Multiple class-action lawsuits have been filed in response to Zoom's security/privacy vulnerabilities and inquiries/concerns from public officials (US Senators Blumenthal, Klobuchar, Bennet, NY Attorney General James, etc.) could lead to an FTC investigation. Zoom's technical response is a positive step and it's engaging directly with officials, yet legal/investigation uncertainties could still divert management bandwidth and hurt the brand.

86. On April 8, 2020, Defendants edited the Security Guide linked on the Company's webpage at https://zoom.us/security. Whereas the Security Guide had formerly identified the ability to "[e]nable an end-to-end (E2E) encrypted meeting" as a pre- and in-meeting security capability, the new version omitted that reference to end-to-end encryption.

87. On April 9, 2020, Morgan Stanley issued an analyst report that discussed the "security overhang" on Zoom's stock, noting that "Zoom has undergone a host of negative publicity as of late, with multiple state AG investigations pending on issues," including "data privacy [and] encryption."

VIII. POST-CLASS PERIOD EVENTS AND ADMISSIONS

88. In the aftermath of the Class Period, analysts continued to cover the fallout from the numerous scandals related to Zoom's privacy and security breaches. In response, school systems and a whole country banned its use. In addition, state attorneys general and the FTC commenced investigations into Zoom's failure to protect users and into false and misleading representations about its privacy and security practices.

A. Zoom Faces Backlash from Its Privacy and Security Breaches

89. On April 17, 2020, Singular Research published a report on Zoom that detailed the impact of privacy and security concerns on Zoom, noting that the New York City Department of Education (overseer of the largest school district in the country) and the Clark County School District in Nevada (which includes Las Vegas) had banned the use of Zoom for remote learning. The report continued: "Similarly, the 'end to end encryption' claimed by Zoom for its calls was misleading. Encryption concerns have already caused customers to curtail Zoom usage and we expect others to follow." The report pointed out that Microsoft, Zoom's main competitor, said that, unlike Zoom, "its Teams platform does not use customer data for ads and encrypts data to protect against cybersecurity threats." The report concluded by stating that, in light of these concerns, "[t]he business advantage generated by the COVID-19 crisis will soon decline":

> - We believe the privacy and security concerns in the recent weeks will lead users to curtail usage of Zoom. We are already seeing these concerns with Zoom bans announced by New York Public Schools and Singapore.
>
> - We think large MNCs such as Microsoft and Cisco pose significant threats to Zoom given their strategic relationships and portfolio breadth. Microsoft Teams is already being recommended as an alternative with better safety and privacy features compared to Zoom.
>
> * * *
>
> Security and privacy concerns could cause permanent reputational damage
>
> The exponential increase in usage of the company's platform has resulted in a spike in security concerns. It has also highlighted several deeper concerns with the underlying security of Zoom's software and the company's practices. These concerns have led to several organizations banning or discouraging its use. Most notably, the New York City Department of Education, which oversees the country's largest public school system, has banned the software outright. The department said that schools should move away from using Zoom as soon as possible and transition to different platforms, such as Microsoft Teams.
>
> The Clark County School District in Nevada has also announced it will disable access to Zoom out of an abundance of caution, while several other districts are reassessing their use of the tool. The security and privacy concerns have piqued the interest of regulators as well as with two U.S. state attorneys general seeking information from Zoom about lapses in its privacy and security. The company is facing lawsuits in New York and California for sharing user data with Facebook.

90. On April 29, 2020, Zacks Equity Research issued an analyst report that detailed the backlash the Company faced from security and privacy shortcomings, stating in relevant part:

> Zoom Video is facing significant backlash from customers due to security issues. Daimler AG, Ericsson, NXP Semiconductors, Bank of America and Tesla are among a host of companies banning or warning employees against using the app due to security concerns. It was also temporarily banned by the New York City Department of Education and Singapore. Moreover, India deemed Zoom Video as an unsafe platform. These allegations revealed a significant chink in Zoom's armor and could prompt customers to shift to more secure platforms like Teams and Webex that are now free to use.
>
> Zoom Video is also struggling with privacy issues. The "zoombombing", which occurs when uninvited individuals disrupt a teleconferencing session, is a major privacy risk. Moreover, the company's iOS app is accused of sending user data to Facebook, which ultimately resulted in a class action lawsuit. The company allegedly overstated its ability to protect users on the platform. It failed to inform users that their communications weren't safeguarded by end-to-end encryption.

91. On May 7, 2020, New York Attorney General Letitia James announced an agreement with Zoom to "implement and maintain a comprehensive data security program to protect all users" and to "enhance its encryption protocols by encrypting users' information, both in transit and as stored online on their cloud servers." The New York Attorney General also listed some of the privacy and data security concerns that led to the agreement, including that "Zoom failed to use AES 256 bit encryption and end-to-end encryption as it had publicly represented"; that Zoom shared user information with Facebook, including from users without Facebook accounts; that certain Zoom users could directly access LinkedIn profiles for other users, even where the unsuspecting users had attempted to remain anonymous by adopting pseudonyms; and that Zoom leaked personal information of some users to others where those users had signed up for Zoom using the same uncommon e-mail domain.

92. On June 9, 2020, at the William Blair Growth Stock Conference, Steckelbert stated that Yuan built Zoom's platform from the ground up:

> Eric, when he started this company, he took many of the talented engineers and spent 2 years building this product from the ground up. So there's a moat in terms of just the lead in which Zoom has in terms of its technology, and again, building it from the ground up so that everything is focused on this purpose of being video first as well as we believe that we have some of the top talent in this space.

B. Zoom Settles FTC Allegations About Misrepresenting Its Security, Privacy and Encryption While the DOJ and SEC Investigate the Same

93. On November 9, 2020, the FTC announced it had entered a proposed consent agreement with Zoom requiring the Company to implement a robust information security program to

settle charges that Zoom engaged in deceptive and unfair practices that undermined the security of its users, including for deceptive end-to-end encryption claims, deceptive claims regarding the level of encryption and deceptive deployment of a web server. The FTC charged Zoom with: falsely or misleadingly representing that it employed end-to-end encryption to secure the content of its videoconferencing users' communication; falsely or misleadingly representing that it used 256-bit encryption to secure the content of communications among participants using Zoom's videoconferencing services; falsely or misleadingly representing that recorded Zoom meetings were immediately stored encrypted in Zoom's cloud storage; installing a web server, without adequate notice to or consent of its users, to circumvent a browser privacy and security safeguard; and omitting to disclose or adequately disclose material information that a Mac update would circumvent Safari's browser privacy and security safeguard and that it would add a web server that would remain on users' computers even after they had uninstalled the Zoom app.

94. The FTC's complaint summarized the allegations as follows:

> Zoom has made numerous, prominent representations touting the strength of the privacy and security measures it employs to protect users' personal information. For example, Zoom has claimed on its website, in Security Guides, and in its privacy policy, that it takes "security seriously," that it "places privacy and security as the highest priority," and that it "is committed to protecting your privacy."
>
> The privacy and security of video communications, including the level of encryption used to secure those communications, is important to users and their decisions about which videoconferencing platform to use, the price to pay for such services, and/or how they use those services. In numerous blog posts, Zoom has pointed to its security as a reason for potential customers to use Zoom's videoconferencing services. In a January 2017 blog post, "Zoom: The Fastest Growing App on Okta," Zoom specifically cited, based on customer feedback, its security feature of "end-to-end AES 256 bit encryption" as important to businesses and one of the reasons for Zoom's growth.
>
> In fact, Zoom did not provide end-to-end encryption for any Zoom Meeting that was conducted outside of Zoom's "Connecter" product (which are hosted on a customer's own servers), because Zoom's servers – including some located in China – maintain the cryptographic keys that would allow Zoom to access the content of its customers' Zoom Meetings.

95. In a November 9, 2020 press release summarizing the allegations and settlement, the FTC stated that "Zoom's misleading claims gave users a false sense of security" and accused Zoom of violating its promises to users:

> Zoom's misleading claims gave users a false sense of security, according to the FTC's complaint, especially for those who used the company's platform to discuss sensitive topics such as health and financial information. In numerous blog posts, Zoom specifically touted its level of encryption as a reason for customers and potential customers to use Zoom's videoconferencing services.
>
> "During the pandemic, practically everyone – families, schools, social groups, businesses – is using videoconferencing to communicate, making the security of these platforms more critical than ever," said Andrew Smith, Director of the FTC's Bureau of Consumer Protection. "Zoom's security practices didn't line up with its promises, and this action will help to make sure that Zoom meetings and data about Zoom users are protected."

96. On December 18, 2020, Zoom filed a current report on SEC Form 8-K regarding a blog post issued the same day titled, "Our Perspective on the DOJ Complaint By Zoom," which disclosed that, commencing in June 2020, the DOJ's U.S. Attorney's Office for the Eastern District of New York had issued grand jury subpoenas seeking information regarding, among other matters, the development and implementation of Zoom's privacy policies. Further, the report on SEC Form 8-K disclosed that in July 2020, the U.S. Attorney's Office for the Northern District of California and the SEC had issued subpoenas seeking information regarding, among other matters, "various security and privacy matters, including Zoom's encryption, and Zoom's statements."

IX. LOSS CAUSATION AND ECONOMIC LOSS

97. During the Class Period, as detailed herein, Defendants made materially false and misleading statements and omissions regarding Zoom's security capabilities, including the ability to use end-to-end AES 256-bit encryption, and the scope of its data collection, handling and use practices. ¶¶27-30, 32, 39, 41-43 and 45-46. These material misrepresentations and omissions caused Zoom's stock price to trade at artificially inflated prices as high as $164.14 on March 23, 2020 and operated as a fraud or deceit on all persons who purchased Zoom's common stock during the Class Period (the "Class"). When Defendants' prior misrepresentations, omissions and fraudulent conduct became apparent to the market, Zoom's stock price declined as the prior artificial inflation came out of the stock price over time. As a result of their purchases of Zoom common stock during the Class Period, Plaintiff and other members of the Class suffered economic loss, *i.e.*, damages, under the federal securities laws.

98. The facts concerning Defendants' false and misleading statements and omissions were revealed to the market through a series of partial disclosures – many mitigated by further false or misleading statements or omissions – beginning with the revelation on July 8, 2019 by security researcher Leitschuh that a vulnerability for Zoom users on Mac computers allowed malicious websites to enable a user's camera without consent and that Defendants had covertly installed a web server on Mac computers, which remained on the computer even if those users uninstalled Zoom. ¶¶35.

99. On this disclosure, Zoom's stock price fell from a closing price of $91.88 on Friday, July 5, 2019, to an intraday low of $89.89 before closing at $90.76 on Monday, July 8, 2019.

100. After Leitschuh's July 8, 2019 article, Defendants continued making false and misleading statements and omissions regarding Zoom's robust security capabilities, including using end-to-end AES 256-bit encryption. *See* ¶¶39, 42-43. Defendants also misrepresented that their Privacy Policy outlined the Company's data collection, handling and use practices and failed to disclose that Zoom's iOS app sent certain user data to Facebook even if Zoom users did not have a Facebook account. ¶¶41, 45-46.

101. On March 30, 2020, *The New York Times* published an article on the New York Attorney General's investigation of Zoom's security and privacy problems, including data sharing with Facebook and flaws that can allow malicious websites to secretly enable users' webcams.

102. On March 30, 2020, Zoom's stock price opened at $160.76 and fell to a low of $147.20 during intraday trading before closing at $150.88 per share.

103. On March 31, 2020, before the market opened, an article in *The Intercept* reported that Defendants' claim that Zoom users could enable end-to-end encryption was "misleading marketing" because the Company did not, in fact, provide end-to-end encryption. The article also reported that a computer science professor at Johns Hopkins called Zoom's representations that end-to-end encryption was available on its platform "slightly dishonest" and said he wished "they just came clean." Indeed, the article stated Defendants admitted: "Currently, it is not possible to enable E2E [end-to-end] encryption for Zoom video meetings," despite having repeatedly represented that users of Zoom's platform could enable end-to-end encryption.

104. On this disclosure, Zoom's stock price fell from a close of $150.88 on March 30, 2020 to close at $146.12 per share on March 31, 2020.

105. On April 1, 2020, Yuan admitted that Zoom had "fallen short" of meeting the Company's and its users' "privacy and security expectations"; said the Company removed the software that shared Zoom user data with Facebook; and referred to Zoom's blog post by Gal, Zoom's Chief Product Officer, which "clarif[ied] the facts" around encryption. Through Gal's April 1, 2020 blog post, Defendants admitted that Zoom meetings were ***not*** capable of using end-to-end encryption and apologized for "incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption." The Company also admitted that its use of the term "end-to-end encryption" conflicted with the commonly accepted definition of the term. ¶¶62-63.

106. Zoom's stock price declined from a close of $146.12 on March 31, 2020 to a low of $135.18 during intraday trading on April 1, 2020 before closing at $137.00.

107. On April 2, 2020, CNBC published an article title, "Zoom falls 11% after CEO apologizes for security lapses, says daily users spiked to 200 million in March," which reported on Yuan's apology for security lapses and noted that "Zoom closed at $121.93 per share, down 11% on the day. Shares of Zoom were down as much as 16% on Thursday morning."

108. On April 2, 2020, *Variety* reported that, in an article published on Yahoo! News titled, "Zoom Suspends Videoconference Feature Development to Fix Privacy, Safety Problems": "Zoom's stock price fell more than 11% Thursday after Yuan's announcement, as the broader market indices were slightly higher. The shares had doubled year-to-date on investor enthusiasm over its prospects amid global stay-at-home environment." Further, the article added that: "The company also admitted that Zoom meetings are not always encrypted end-to-end. In a post attempting to 'clarify' the issue, it noted that data cannot be encrypted on devices that don't use Zoom's proprietary communication protocol (such as phones or certain room-based videoconferencing systems)."

109. Zoom's stock price continued to decline from a close of $137.00 on April 1, 2020 to a low of $114.50 during intraday trading on April 2, 2020 before closing at $121.93.

110. On April 2, 2020 after market close, *The New York Times* published an article about unnecessary data disclosures from a data-mining feature on Zoom that allowed participants to secretly snoop on other users' LinkedIn profile data. The article reported that an assistant professor of computer science and public affairs at Princeton University said: "It's very clear that they have not prioritized privacy and security in the way they should have, which is obviously more than a little concerning," and that, though Defendants had made the data-mining feature available in 2018, it was not disclosed in Zoom's Privacy Policy or terms of service.

111. On April 3, 2020 during intraday trading, Citizen Lab reported that Zoom used non-industry-standard cryptographic techniques with identifiable weaknesses; that, contrary to Zoom's representations, the Company uses AES 128-bit encryption, not 256-bit encryption, and that the encryption is generated at times from servers located in China; and that Zoom does not use end-to-end encryption. Multiple news organizations covered the report. ¶¶71-73. On the same day, Defendants published a response to Citizen Lab's report in which Yuan "recogniz[ed] that we can do better with our encryption design."

112. Zoom's stock price declined from a close of $121.93 on April 2, 2020 to a low of $120.11 during intraday trading on April 3, 2020 in response to the April 2, 2020 article in *The New York Times*, the April 3, 2020 Citizen Lab report and Defendants' response thereto.

113. On April 4, 2016, *The Wall Street Journal* published an article based on an interview with Yuan in which he stated that end-to-encryption would not be available for a few months. The articles noted that there was a backlash not just from security professions but also from corporate users like Tesla and Space Ex, which had stopped using Zoom's platform based on its security vulnerabilities. Yuan said to *The Wall Street Journal* that: "If we mess up again, it's done" and that: "I really messed up as CEO, and we need to win their trust back. This kind of thing shouldn't have happened."

114. On April 6, 2020, Credit Suisse issued an analyst report noting: "Encryption concerns have already caused some high profile customers to curtail Zoom usage . . . and we expect others could follow . . . ." On the same date, *Fortune* published an article titled, "Zoom stock down after schools and businesses banned the meeting app over 'Zoom bombing' security issues," which

reported that the Company's stock price had declined by 14.5% after security concerns, including reports that Zoom's claim that it used end-to-end encryption were misleading, leading organizations to ban or discourage the platform's use: "Zoom stock dropped as much as 14.5% this morning, after concerns over the security of the company's video-chat and meeting software led to several major organizations banning or discouraging its use."

115. Zoom's stock price declined from a close of $128.20 on April 3, 2020 to a low of $108.53 during intraday trading on April 6, 2020 before closing at $122.94.

116. The timing and magnitude of the declines in Zoom's stock prices reflected in ¶¶15, 53-55, 61, 64, 76-78 above negates any inference that the loss suffered by Plaintiff and other Class members was caused by changed market conditions, macroeconomic or industry factors or Company-specific facts unrelated to Defendants' fraudulent conduct.

117. The economic loss, *i.e.*, damages, suffered by Plaintiff and other members of the Class was a direct and proximate result of Defendants' misrepresentations, artificially inflating Zoom's common stock price, and the subsequent significant declines in the value of Zoom common stock as the true state of the Company's operations was revealed to the market in a series of partial disclosures correcting the misrepresentations or revealing the economic impact thereof.

X. APPLICABILITY OF FRAUD ON THE MARKET AND *AFFILIATED UTE* PRESUMPTION OF RELIANCE

118. Plaintiff will rely upon the presumption of reliance established by the fraud-on-the-market doctrine in that, among other things:

(a) Defendants made public misrepresentations or failed to disclose material facts during the Class Period;

(b) The omissions and misrepresentations were material;

(c) The Company's stock traded in an efficient market;

(d) The misrepresentations alleged would tend to induce a reasonable investor to misjudge the value of the Company's stock; and

(e) Plaintiff and other members of the Class purchased Zoom common stock between the time Defendants misrepresented or failed to disclose material facts and the time the facts were disclosed, without knowledge of the misrepresented or omitted facts.

119. At all relevant times, the market for Zoom's common stock was efficient for the following reasons, among others:

(a) As a regulated issuer, Zoom filed periodic public reports with the SEC;

(b) Zoom's stock traded on the NASDAQ; and

(c) Zoom regularly communicated with public investors via established market communication mechanisms, including through regular dissemination of press releases on the major news wire services and through other wide-ranging public disclosures, such as communications with the financial press, securities analysts and other similar reporting services.

120. Plaintiff will also rely upon the presumption of reliance under *Affiliated Ute Citizens v. United States*, 406 U.S. 128 (1972), for the claims asserted herein against Defendants that are predicated upon omissions of material fact for which there was a duty to disclose.

XI. CLASS ACTION ALLEGATIONS

121. Plaintiff brings this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of all members of the Class. Excluded from the Class are Defendants and their families and directors and officers of Zoom and their families and affiliates.

122. The members of the Class are so numerous that joinder of all members is impracticable. The disposition of their claims in a class action will provide substantial benefits to the parties and the Court. Zoom has 48.69 million shares of common stock outstanding.

123. There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class that predominate over questions that may affect individual Class members include:

(a) Whether the Exchange Act was violated by Defendants;

(b) Whether Defendants omitted or misrepresented material facts;

(c) Whether Defendants' statements omitted material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading;

(d) Whether Defendants knew, or were deliberately reckless in not knowing, that their statements were false and misleading;

(e) Whether the price of Zoom's common stock was artificially inflated; and

(f) The extent of damage sustained by Class members and the appropriate measure of damages.

124. Plaintiff's claims are typical of those of the Class because Plaintiff and the Class sustained damages from Defendants' wrongful conduct.

125. Plaintiff will adequately protect the interests of the Class and has retained counsel experienced in class action securities litigation. Plaintiff has no interests that conflict with those of the Class.

126. A class action is superior to other available methods for the fair and efficient adjudication of this controversy.

COUNT I

For Violation of §10(b) of the Exchange Act and Rule 10b-5 Promulgated Thereunder (Against All Defendants)

127. Plaintiff incorporates ¶¶1-126 by reference.

128. During the Class Period, Defendants disseminated or approved the false statements specified above, which they knew, or were deliberately reckless in not knowing, were misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

129. Defendants violated §10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder in that they:

(a) Employed devices, schemes and artifices to defraud;

(b) Made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or

(c) Engaged in acts, practices and a course of business that operated as a fraud or deceit upon Plaintiff and others similarly situated in connection with their purchases of Zoom common stock during the Class Period.

130. Plaintiff and the Class have suffered damages in that, in reliance on the integrity of the market, they paid artificially inflated prices for Zoom's common stock. Plaintiff and the Class would not have purchased Zoom common stock at the prices they paid, or at all, if they had been aware that the market prices had been artificially and falsely inflated by Defendants' misleading statements.

131. As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and the other members of the Class suffered damages in connection with their purchases of Zoom common stock during the Class Period.

COUNT II

For Violation of §20(a) of the Exchange Act (Against the Individual Defendants)

132. Plaintiff incorporates ¶¶1-131 by reference.

133. The Individual Defendants acted as controlling persons of Zoom within the meaning of §20(a) of the Exchange Act. By virtue of their positions and their power to control public statements about Zoom, the Individual Defendants had the power and ability to control the actions of Zoom and its employees. Zoom controlled the Individual Defendants and its other officers and employees. By reason of such conduct, Defendants are liable pursuant to §20(a) of the Exchange Act.

XII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief and judgment as follows:

A. Determining that this action is a proper Class action, having designated Plaintiff as Lead Plaintiff, and certifying Plaintiff as Class representative under Rule 23 of the Federal Rules of Civil Procedure and Plaintiff's counsel as Lead Counsel;

B. Awarding compensatory damages in favor of Plaintiff and the other Class members against all Defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Awarding Plaintiff and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

D. Awarding such equitable, injunctive or other relief as may be deemed appropriate by the Court.

XIII. JURY DEMAND

Plaintiff demands a trial by jury.

DATED: December 23, 2020

ROBBINS GELLER RUDMAN
& DOWD LLP
SHAWN A. WILLIAMS
MATTHEW S. MELAMED
JOHN H. GEORGE
ARMEN ZOHRABIAN

s/ Shawn A. Williams
SHAWN A. WILLIAMS

Post Montgomery Center
One Montgomery Street, Suite 1800
San Francisco, CA 94104
Telephone: 415/288-4545
415/288-4534 (fax)
shawnw@rgrdlaw.com
mmelamed@rgrdlaw.com
jgeorge@rgrdlaw.com

Lead Counsel for Lead Plaintiff

CERTIFICATE OF SERVICE

I hereby certify under penalty of perjury that on December 23, 2020, I authorized the electronic filing of the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses on the attached Electronic Mail Notice List, and I hereby certify that I caused the mailing of the foregoing via the United States Postal Service to the non-CM/ECF participants indicated on the attached Manual Notice List.

s/ Shawn A. Williams
SHAWN A. WILLIAMS

ROBBINS GELLER RUDMAN
& DOWD LLP
Post Montgomery Center
One Montgomery Street, Suite 1800
San Francisco, CA 94104
Telephone: 415/288-4545
415/288-4534 (fax)
E-mail: shawnw@rgrdlaw.com

Mailing Information for a Case 3:20-cv-02353-JD Drieu v. Zoom Video Communications, Inc. et al

Electronic Mail Notice List

The following are those who are currently on the list to receive e-mail notices for this case.

- **Jenna C. Bailey**
  jbailey@cooley.com,jcorrell@cooley.com
- **John Hamilton George**
  jgeorge@rgrdlaw.com
- **Patrick Edward Gibbs**
  pgibbs@cooley.com,bgiovannoni@cooley.com
- **Reza John Harris**
  rjharris@cooley.com
- **Benjamin Heikali**
  Bheikali@faruqilaw.com,ealdo@faruqilaw.com,rglezakos@faruqilaw.com,ecf@faruqilaw.com,tpeter@faruqilaw.com
- **Joseph Alexander Hood , II**
  ahood@pomlaw.com
- **Phillip C Kim**
  pkim@rosenlegal.com,pkrosenlaw@ecf.courtdrive.com
- **Jeremy A. Lieberman**
  jalieberman@pomlaw.com,tcrockett@pomlaw.com,disaacson@pomlaw.com,abarbosa@pomlaw.com,lpvega@pomlaw.com
- **Matthew Seth Melamed**
  mmelamed@rgrdlaw.com,smorris@rgrdlaw.com,e_file_SD@rgrdlaw.com,smorris@ecf.courtdrive.com
- **Danielle Suzanne Myers**
  dmyers@rgrdlaw.com,dmyers@ecf.courtdrive.com,e_file_sd@rgrdlaw.com
- **Jennifer Pafiti**
  jpafiti@pomlaw.com,jalieberman@pomlaw.com,ahood@pomlaw.com,egoodman@pomlaw.com,disaacson@pomlaw.com,ashmatkova@pomlaw.com,abarbosa@pomla
- **Laurence Matthew Rosen**
  lrosen@rosenlegal.com,larry.rosen@earthlink.net,lrosen@ecf.courtdrive.com
- **Juan Carlos Sanchez**
  jsanchez@rgrdlaw.com
- **Jessica Valenzuela Santamaria**
  jsantamaria@cooley.com,galancr@cooley.com
- **Craig Edward TenBroeck**
  ctenbroeck@cooley.com,maraujo@cooley.com,efiling-notice@ecf.pacerpro.com
- **Tamar A Weinrib**
  taweinrib@pomlaw.com,egoodman@pomlaw.com
- **Shawn A. Williams**
  shawnw@rgrdlaw.com,cbarrett@rgrdlaw.com,ShawnW@ecf.courtdrive.com,e_file_sd@rgrdlaw.com
- **Armen Zohrabian**
  AZohrabian@rgrdlaw.com,azohrabian@ecf.courtdrive.com

Manual Notice List

The following is the list of attorneys who are **not** on the list to receive e-mail notices for this case (who therefore require manual noticing). You may wish to use your mouse to select and copy this list into your word processing program in order to create notices or labels for these recipients.

- (No manual recipients)